REMARKS

The amendments to claims 1 and 9 are made in the light of prior art document U.S. Patent No. 5,412,730 to Jones and the reasons are as follows:

It is important to note that an essential feature of the method of the '730 Patent is that the advancing of each of pseudo-random number generators 23, 27 is dependent on a count of the data being transmitted. This, in transmitting station 11, block counter 21 counts the data provided by data source 15, and when the count reaches an interval number provided to counter 21, counter 21 sends an advance instruction to pseudo-random number generator 23, which in response supplies a new encryption/decryption key to encryptor 17. Similarly, in receiving station 12, block counter 29 counts the received decrypted data provided by decryptor 31, and when the count reaches the same interval number also provided to counter 29, counter 29 sends an advance instruction to pseudo-random number generator 27, which in response supplies the same new encryption/decryption key to decryptor 31.

It will be seen that encryptor 17 and decryptor 31 are synchronized or kept in step by counting the transmitted data, i.e., only when a predetermined amount of data has been counted as encrypted at the transmit end does encryptor 17 step to the next encryption/decryption key, and only when the same predetermined amount of data has been counted as decrypted at the receive end does decryptor 31 step to the same next encryption/decryption key. It is in this manner that U.S. Patent No. 5,412,730 ensures that encryptor 17/decryptor 31 use the same encryption/decryption key of the succession of encryption/decryption keys to encrypt/decrypt the same data.

It is to be realized that it is essential/crucial to the method of the '730 Patent that there is monitored the count or some other predetermined characteristic of the transmitted data. This is

because in the '730 Patent, for security purposes, it is an object to avoid the need to add additional synchronization information to the transmitted data. In other words, because no additional synchronization information is permitted, synchronization must be achieved in some way through use of the transmitted data itself. In this matter, the Examiner's attention is directed to the '730 Patent, col. 1, lines 48-59, which part of the '730 Patent ends by saying: "In this way, no additional synchronisation information needs to be added to the data stream." As regards it being essential to the method of the '730 Patent that there is monitored a predetermined characteristic of the transmitted data, please also see claim 1 of the'730 Patent which specifies dependency "upon a predetermined characteristic of the data being transmitted".

The dependency on the data being transmitted is a major disadvantage in the '730 Patent, due to the consequent vulnerability of the method to inaccuracy in data transmission. Thus, if there is loss or corruption of data during transmission, this will destroy synchronization -- the method of the '730 Patent does not have the ability to maintain synchronicity in the event of inaccuracy in data transmission. In this regard, the Examiner's attention is directed to the first sentence of the abstract of the '730 Patent, which mentions suitability "for transmitting encrypted data over a voice-grade telephone line". In the case of a "voice-grade telephone line", accuracy of data transmission is very high. This is to be contrasted to data transmission over the Internet or in mobile phone communication -- the method of the '730 Patent would be completely unsuited to such applications.

The invention of the present application is not dependent on the data being transmitted, and consequently does have the capability of maintaining synchronicity in the event of inaccuracy in data transmission. In this regard, claim 1 now specifies that the first and second cipher

generators are signaled to cause them to generate the next cipher in the sucession of ciphers, and that *the derivation of this signaling is independent of the information being transmitted.* In the present application, in the case of the communication system described by way of example, a pulse Co1 signals to both the first and second cipher generators 3, 35, the receipt of a new message Mp for transmission. This causes cipher generators 3, 35 to generate a new cipher to securely transmit the new message. This new cipher is then used until a further pulse Co1 signals the receipt of the next message Mp for transmission. Thus, it can be seen that in no way is a predetermined characteristic or count of the actual data transmitted involved in the derivation of signal Co1 -- the derivation is independent of any characteristic or count of the actual data transmitted.

It is to be appreciated that the teaching of the '730 Patent is contrary to the present invention. The '730 Patent teaches maintaining synchronicity by reliance only on the data *per se* being transmitted and the '730 Patent teaches against the use of additional signals to maintain synchronicity. In the present invention, synchronicity is maintained without use of the actual data being transmitted, and by means of additional signaling.

Wherefore, a favorable action is earnestly solicited.

Respectfully submitted,

KIRSCHSTEIN, OTTINGER, ISRAEL & SCHIFFMILLER, P.C.
Attorneys for Applicant(s)
489 Fifth Avenue
New York, New York 10017-6105
Tel: (212) 697-3750
Fax: (212) 949-1690

Alan Israel
Reg. No. 27,564